changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation. The Protected CII Program Manager or the Protected CII Program Manager's designees shall inform the submitter when a change in status is made. Notice of the change in status of Protected CII shall be provided to all recipients of that Protected CII under § 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times by appropriate storage and handling. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Use and storage.* When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons. When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity.

(c) *Reproduction.* Pursuant to procedures prescribed by the Protected CII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(d) *Disposal of information.* Documents and material containing Protected CII may be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by secure means of delivery as determined by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(f) *Automated Information Systems.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall establish security requirements for Automated Information Systems that contain Protected CII.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for IAIP, or the Under Secretary's designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority. Any disclosure or use of Protected CII within the Federal government is limited by the terms of the CII Act of 2002. Accordingly, any advisories, alerts, or warnings issued to the public pursuant to paragraph (e) of this section shall protect from disclosure:

(1) The source of any voluntarily submitted CII that forms the basis for the warning, and

(2) Any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(b) *Federal, State, and local government sharing.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to an employee of the Federal government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written